1. References.

[1] A. Kalafut, A. Acharya, and M. Gupta.(2006), *A study of malware in peer-to-peer networks*. In ACMSIGCOMM conference on Internet measurement.

[2] A. Niculescu-Mizil and R. Caruana.(2005), *Predicting good probabilities with supervised learning*. In International Conference on Machine Learning (ICML).

[3] A. Ta-Shma and U. Zwick .(2007), *Deterministic rendezvous, treasure hunts and strongly universal exploration sequences*. Proc. 18th ACM-SIAM Symposium on Discrete Algorithms, 599-608.

[4] ADAM P.F. CHAUDHURI, A., AND FOSTER, J.S. (2009), *SCanDroid: Automated Security Certification of Android Applications*, Submitted to IEEE Symposium of Security and Privacy.

[5] Aickelin, U., Greensmith, J., and Twycross, J.(2004) ,*Immune System Approaches to Intrusion Detection—a Review*. In the Proceeding of the Third International Conference on Artificial Immune Systems(ICARIS–04), pp.316–329.

[6] Amaral LA, Scala A, Barthelemy M, Stanley HE. (2000), *Classes of small-world networks*. Proc Natl Acad Sci U S A 97: 11149-52.

[7] Anirudh Ramachandran, Nick Feamster.(2006), *Understanding the network level behaviour of spammers*, SIGCOMM 06,Pisa, Italy, 291-302.

[8] Anirudh Ramachandran, David Dagon, Nick Feamste.(2006), *Can DNS-based Blacklists keep up with Bots*,CA, USA.

[9] B. Zhang, J. Yin, J. Hao, D. Zhang, and S.Wang.(2007), *Malicious codes detection based on ensemble learning*. In Autonomic and Trusted Computing (ATC).

[10] Barse, E., Kvarnstrom, H. & Jonsson, E. (2003), *Synthesizing Test Data for Fraud Detection Systems*. Proc. of the 19th Annual Computer Security Applications Conference, pp 384-395.

[11] Bauke H, Sherrington D (2007), *Topological phase transition in complex networks*. arxiv.org/abs/0710.0831.

[12] Bebek G, Berenbrink P, Cooper C, Friedetzky T, Nadeau J, et al (2006), *The degree distribution of the generalized duplication model*. Theoretical Computer Science 369: 239-249.

[13] BOSE, A., HU, X., SHIN, K.G., AND PARK, T. (2008), *Behavioral detection of malware on mobile handsets*. In Proceeding of the 6th international Conference on Mobile Systems, Applications, and Services.

[14] BUENNEMEYER, T.K., ET AL, (2008), *Mobile device profiling and intrusion detection using smart batteries*. International Conference on System Sciences, pp.296-296.

[15] Calton pu, Steve webb.(2006), *Observed trends in spam construction techniques: A case study of spam evolution*,pp 104-112.

[16] Caruana, R. & Niculescu-Mizil, A. (2004). *Data Mining in Metric Space: An Empirical Analysis of Supervised Learning Performance Criteria*. Proc. of SIGKDD04,pp 69-78.

[17] Chen BL, Hall DH, Chklovskii DB. (2006), *Wiring optimization can relate neuronal structure and function*. Proc Natl Acad Sci U S A 103: 4723{4728}.

[18] Chen, R., Chiu, M., Huang, Y. & Chen, L. (2004), *Detecting Credit Card Fraud by Using Questionaire-Responded Transaction Model Based on Support Vector Machines*. Proc. of IDEAL2004,pp 800-806.

[19] CHAUDHURI, A. (2009), *Language-Based Security on Android. ACM Workshop on Programming Languages and Analysis for Security* (PLAS), pp. 1–7.

[20] Chiu, C. & Tsai, C. (2004). A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Proc. of 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service.

[21] Cynthia et al.(2007), *Charecterizing spam traffic and spammers to appear in proc of ICCIT-2007*, Gyoungju, South Korea.

[22] D. Bilar.(2007), *Opcode as predictors for malware*. International Journal of Electronic Security and Digital Forensics, 1(2).

[23] D. Bruschi, L. Martignoni, and M. Monga.(2007), *Code normalization for self-mutating malware*, IEEE Security and Privacy, vol. 5, no. 2, pp. 46–54.

[24] D. K. S. Reddy and A. K. Pujari.(2006), *N-gram analysis for computer virus detection*. Journal in Computer Virology, 2(3).

[25] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar and Y. Elovici. (2006), *Application of Artificial Neural Networks Techniques to Computer Worm Detection*, Proc. International Joint Conference on Neural Networks, Vancouver.

[26] DAGON, C., MARTIN, T., AND STARNER, T. (2004), *Mobile phones as computing devices the viruses are coming. Pervasive Computing*, pp. 11-15.

[27] Dalvi, N., Domingos, P., Mausam, Sanghai, P. & Verma, D. (2004), *Adversarial Classification*. Proc.of SIGKDD04,pp 99-108.

[28] Delgrande, J. P., Schaub, T., and Tompits, H. (2003), *A Framework for Compiling Preferences in Logic Programs. Theory and Practice of Logic Programming 3*, 2, 129– 187.

[29] Dhinaharan Nagamalai, Cynthia.D, Jae Kwang Lee.(2007). *A Novel Mechanism to defend DDoS attacks caused by spam*, International Journal of Smart Home, SERSC, Seoul, pp 83-96.

[30] E. Carrera and G. Erd´elyi,(2010), *Digital genome mapping-advanced binary malware analysis*, in Virus Bulletin Conference.

[31] E. Kranakis, D. Krizanc, P. Morin.(2008), *Randomized Rendez-Vous with Limited Memory*, Proc. 8th Latin American Theoretical Informatics, Springer LNCS 4957,pp 605-616.

[32] Eiter, T., Ianni, G., Schindlauer, R., and Tompits, H. (2005) , *A Uniform Integration of Higher-Order Reasoning and External Evaluations in Answer-Set Programming.* In Proceedings of the Nineteenth International Joint Conference on Artificial Intelligence. Morgan Kaufmann.

[33] Fan, W. (2004), *Systematic Data Selection to Mine Concept-Drifting Data Streams*. Proc. of SIGKDD04,pp 128-137.

[34] Faber, W., Leone, N., and Pfeifer, G. (2004), *Recursive Aggregates in Disjunctive Logic Programs: Semantics and Complexity*. In Proceedings of the Ninth European Conference on Logics in Artificial Intelligence (JELIA 2004), J. J. Alferes and J. A. Leite, Eds. LNCS, subseries LNAI, vol. 3229. Springer, 200–212.

[35] Fang Hao, Murali Kodialam, T.V. Lakshman, Hui Zhang. (2005), *Fast Payload Based Flow Estimation for Traffic Monitoring and Network Security*.

[36] Fulu Li, Mo-han Hsieh.(2006). *An empirical study of clustering behavior of spammers and Group based Anti-spam strategies*, CEAS 2006, pp 21-28.

[37] G. McGraw and G. Morrisett.(2001), *Attacking malicious code: report to the Infosec research council*. IEEE Software, 17(5), pp 33 - 41.

[38] H. Flake.(2004), *Structural comparison of executable objects*, in Proceedings of the IEEE Conference on Detection of Intrusions, Malware and Vulnerability Assessment (DIMVA), pp.161–173.

[39] H. Lee, W. Kim, M. Hong. (2004),*Artificial Immune System against Viral Attack*, ICCS 2004, Lecture Notes in Computer Science 3037, pp. 499-506.

[40] I. Briones and A. Gomez.(2008), *Graphs, entropy and grid computing: Automatic comparison of malware*, in Proceedings of the 2008 Virus Bulletin Conference, pp 61 - 68.

[41] I. Stamatopoulou . (2008), *A Formal Framework for the Modelling of Multi-Agent Systems with Dynamic Structure*. Ph.D. thesis, University of Sheffield, UK.

[42] J. Gordon.(2004), L*essons from virus developers*: The Beagle worm history.

[43] K. Wang and S. Stolfo.(2005), *Anomalous payload-based worm detection and signature generation*. In Recent Advances in Intrusion Detection (RAID).

[44] K. P. Anchor, P. D. Williams, G. H. Gunsch et al. (2002), *The Computer Defense Immune System: Current and Future Research in Intrusion Detection*, Evolutionary Computation,pp. 1027-1032.

[45] Kao, D.-Y., Wang, S.-J., Huang, F. F.-Y., Bhatia, S., & Gupta, S. (2008), *Dataset Analysis of Proxy Logs Detecting to Curb Propagations in Network Attacks*. Paper presented at the ISI 2008 Workshops.

[46] L. Gasieniec, A. Pelc, T. Radzik, X. Zhang.(2007), *Tree exploration with logarithmic memory*, Proc. 18th Annual ACM-SIAM Symposium on Discrete Algorithms,pp 585-594.

[47] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson.(2004), *CSI/FBI computer crime and security survey. Technical report*, Computer Security Institute.

[48] Liu, Z., Wang, C. & Chen, S.(2008),Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling, IEEE Computer Society, 214-219, 2008.

[49] M. Bailey, E. Cooke, F. Jahanian, D. Watson, and J. Nazario.(2005), *The Blaster Worm: Then and Now*. In Security & Privacy, Volume 3 Issue 4, pages 26-31

[50] M. Christodorescu and S. Jha.(2004), Testing malware detectors. In Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis 2004 (ISSTA'04), pages 34-44, Boston, MA, USA.

[51] M. Ester, H.-P. Kriegel, J. S, and X. Xu.(2001), *A density-based algorithm for discovering clusters in large spatial databases with noise*, in Proceedings of 2nd International Conference of Knowledge Discovery and Data Mining, pp. 226–231.

[52] M. G. Kang, P. Poosankam, and H. Yin. Renovo.(2007), *A hidden code extractor for packed executables. In WORM '07*: Proceedings of the 5th ACM Workshop on Recurring Malcode.

[53] Mihai Christodorescu , Somesh Jha , Sanjit A. Seshia , Dawn Song , Randal E. Bryant.(2005),*Semantics-Aware Malware Detection*, Proceedings of the 2005 IEEE Symposium on Security and Privacy, pp.32-46.

[54] Nodine, M., Ngu, A., Cassandra, A., and Bohrer, W. (2003), *Scalable Semantic Brokering over Dynamic Heterogeneous Data Sources* in InfoSleuth. IEEE Transactions on Knowledge and Data Engineering 15, 5, 1082–1098.

[55] O. Reingold .(2008) *Undirected connectivity in log-space.* Journal of the ACM,pp 1-24.

[56] P. Flocchini, G. Prencipe, N. Santoro, P. Widmayer.(2010), *Gathering of asynchronous oblivious robots with limited visibility*, Proc. 18th Annual Symposium on Theoretical Aspects of Computer Science,pp 247-258.

[57] P. Fogla, M. Sharif, R. Perdisci, O. M. Kolesnikov, andW. Lee.(2006), *Polymorphic blending attack*. In USENIX Security Symposium.

[58] P. Kabiri and A.A. Ghorbani. (2005), *Research on intrusion detection and response: A survey*, International Journal of Network Security, pp. 84-102.

[59] P. Szor and P. Ferrie.(2001), *Hunting for metamorphic*. In Proceedings of the 2001 Virus Bulletin Conference (VB2001), pp 123-144.

[60] P. S. Deng, J. Wang, W. Shieh et al. (2003), *Intelligent automatic malicious code signatures extraction*, IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, pp. 600-603.

[61] R. Lyda and J. Hamrock (2007), *Using entropy analysis to find encrypted and packed malware*. IEEE Security and Privacy, pp.40–45.

[62] R. O. Duda, P. E. Hart, and D. G. Stork.(2000), *Pattern Classification (2nd Edition)*. Wiley-Interscience,ch. 10, pp. 517–598.

[63] R. Perdisci, A. Lanzi, and W. Lee.(2008), *Classification of packed executables for accurate computer virus detection*. Patter Recognition Letters, 29(14):1941–1946, 2008.

[64] R. Perdisci, G. Gu, and W. Lee.(2006), *Using an ensemble of oneclass svm classifiers to harden payload-based anomaly detectionsystems*. In International Conference on Data Mining (ICDM).

[65] Rafael H. Bordini, Jomi Fred Hubner, and Michael Wooldridge. (2007), *Programming Multi-Agent Systems in AgentSpeak* using Jason. John Wiley & Sons Ltd.

[66] S. Bradde, A. Braunstein, H. Mahmoudi, F. Tria, M. Weigt, and R. Zecchina.(2009), *Aligning graphs and finding substructures by message passing*, pp 34-41.

[67] Shishir Kumar, Durgesh Pant.(2009), *Detection and Prevention of New and Unknown Malware using Honeypots*. International Journal on Computer Science and Engineering Vol.1,pp 56-61.

[68] Vladimir Mijatovic.(2004) , *Mechanism for detecting and prevention of email spamming*, Peer to Peer and SPAM in the Internet Raimo Kantola's technical report, 135-145, 2004.

[69] Victoria J. Hodge, Jim Austin. (2004), *A Survey of Outlier Detection Methodologies*. Artif. Intell.(2004), pp 85-126

[70] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod. (2003), *The link between AIS and IDS.* In Proc. of the 2nd International Conference on Artificial Immune Systems (ICARIS). LNCS 2787, pp. 147-155.

[71] YAP, T.S., AND EWE, H.T. (2005). A mobile phone malicious software detection model with behavior checker. Lecture Notes in Computer Science, 3597:57-65.

[72] ZHANG, X., ACIIÇMEZ, O., AND SEIFERT, J.P. (2007). *A Trusted Mobile Phone Reference Architecture via Secure Kernel*. In Proceedings of the ACM workshop on Scalable Trusted Computing, pp. 7–14.

[73] Zhenhe Guo, Zhengkai Liu, Ying Tan, Ling Zhang(2006) , *An NNbased Malicious Executables Detection Algorithm Based on Immune Principles*, pp.5–6.

Signature of Student

Mr. Pradeep Pundir

Signature of Research Guide

Dr. Virendra Gomase